IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Kenta HORI

Batch:

Serial No.: NEW APPLICATION

Group Art Unit:

Filed: December 3, 2001

Examiner:

For: METHOD AND PROGRAM FOR PREVENTING UNFAIR USE OF SOFTWARE

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following country is hereby requested for the above-identified application and the priority provided in 35 U.S.C. § 119 is hereby claimed:

JAPAN 2000-370630 December 5, 2000

In support of this claim, a certified copy of said original foreign application is filed herewith. It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

12-03-01
Date

Marc A. Rossi
Registration No. 31,923

Attorney Docket: IIZU:011

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２０００年１２月　５日

出願番号
Application Number:　特願２０００－３７０６３０

出願人
Applicant(s):　堀　健太

２００１年１１月１６日

特許庁長官
Commissioner,
Japan Patent Office　及川耕造

出証番号　出証特２００１－３０９９９６１

【書類名】　特許願
【整理番号】　P0012
【あて先】　特許庁長官　及川　耕造　殿
【国際特許分類】　G09C　5/00
【発明者】
　【住所又は居所】　神奈川県相模原市古淵一丁目２３番９号
　【氏名】　堀　健太
【特許出願人】
　【住所又は居所】　神奈川県相模原市古淵一丁目２３番９号
　【氏名又は名称】　堀　健太
【代理人】
　【識別番号】　100077539
　【弁理士】
　【氏名又は名称】　飯塚　義仁
　【電話番号】　03-5802-1811
【手数料の表示】
　【予納台帳番号】　034809
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ソフトウエアの不正利用防止方法及び記憶媒体

【特許請求の範囲】

【請求項１】　ユーザーのコンピュータのファイルシステムの特徴を検出し、検出したファイルシステムの特徴に基づき固有情報を生成する第１のステップと、

前記第１のステップで生成した固有情報に基づきソフトウエアのライセンス提供者の側でキーデータを生成し、該キーデータを前記ユーザに提供する第２のステップと、

前記ソフトウエアを利用しようとするコンピュータのファイルシステムの特徴を検出し、検出したファイルシステムの特徴に基づき固有情報を生成する第３のステップと、

前記キーデータに対応する前記ファイルシステムの特徴に基づく固有情報と前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報との一致若しくは類似性に基づき前記ソフトウエアの利用可否を判定する第４のステップと

を具備するソフトウエアの不正利用防止方法。

【請求項２】　前記ユーザに提供された前記キーデータから前記ファイルシステムの特徴に基づく固有情報を復元するステップを具備し、

前記第４のステップでは、前記復元されたファイルシステムの特徴に基づく固有情報と前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報とを比較し、両情報の一致若しくは類似性に基づき前記ソフトウエアの利用可否を判定する請求項１に記載のソフトウエアの不正利用防止方法。

【請求項３】　前記第２のステップでは、所定の変換アルゴリズムに従って前記ファイルシステムの特徴に基づく固有情報を前記キーデータに変換し、

前記固有情報を復元するステップでは、前記所定の変換アルゴリズムの逆変換によって、前記キーデータから前記ファイルシステムの特徴に基づく固有情報を復元する請求項２に記載のソフトウエアの不正利用防止方法。

【請求項４】　前記第１及び第３のステップにおいて、コンピュータのファ

イルシステム情報を読み取ることにより前記ファイルシステムの特徴を検出する請求項１乃至３のいずれかに記載のソフトウエアの不正利用防止方法。

【請求項５】　前記第４のステップでは、前記キーデータに対応する前記ファイルシステムの特徴に基づく固有情報と前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報との差分を計算し、この差分の大きさに応じて前記ソフトウエアの利用可否を判定する請求項１乃至４のいずれかに記載のソフトウエアの不正利用防止方法。

【請求項６】　前記第４のステップは、前記ソフトウエアを前記コンピュータにインストールするとき、あるいは、前記ソフトウエアを前記コンピュータで起動するとき、あるいは、前記ソフトウエアを前記コンピュータでコピーしようとするとき、のいずれか少なくとも１つの時点で実行され、該第４のステップで利用不可と判定されたならばその利用を禁止する請求項１乃至５のいずれかに記載のソフトウエアの不正利用防止方法。

【請求項７】　前記第２のステップでユーザに提供された前記キーデータを保存するステップと、

前記第４のステップで前記ソフトウエアが利用可と判定されたことを少なくとも一つの条件として、前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報に適合するように前記保存されたキーデータの内容を更新するステップと

を更に具備する請求項１乃至６のいずれかに記載のソフトウエアの不正利用防止方法。

【請求項８】　コンピュータ読み取り可能な記憶媒体であって、コンピュータのソフトウエアの不正利用を防止する方法を前記コンピュータに実行させるためのプログラムを記憶しており、このプログラムは、

ユーザーのコンピュータのファイルシステムの特徴を検出し、検出したファイルシステムの特徴に基づく固有情報を出力する第１のステップであって、これにより、該ファイルシステムの特徴に基づく固有情報が前記ソフトウエアのライセンス提供者に対して送付されて該ライセンス提供者の側で該固有情報に対応する固有のキーデータが生成されることを可能にすることと、

前記生成されたキーデータを前記ライセンス提供者の側から受け取る第２のステップと、

前記ソフトウエアを利用しようとするコンピュータのファイルシステムの特徴を検出し、検出したファイルシステムの特徴に基づき固有情報を生成する第３のステップと、

前記キーデータに対応する前記ファイルシステムの特徴に基づく固有情報と前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報との一致若しくは類似性に基づき前記ソフトウエアの利用可否を判定する第４のステップと

を具備する。

【請求項９】　前記プログラムは、前記第２のステップでユーザに提供された前記キーデータを保存するステップと、前記第４のステップで前記ソフトウエアが利用可と判定されたことを少なくとも一つの条件として、前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報に適合するように前記保存されたキーデータの内容を更新するステップとを更に具備する請求項８に記載の記録媒体。

【請求項１０】　第１のステップでは、前記ファイルシステムの特徴に基づく固有情報をネットワークを介して前記ソフトウエアのライセンス提供者に対して送付し、前記第２のステップでは、前記ライセンス提供者の側で生成された前記キーデータをネットワークを介して受け取る請求項８又は９に記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ソフトウエアの不正利用防止方法及び該方法に係るプログラムを記憶した記憶媒体に関し、特に、ソフトウエアを正規に利用する特定のコンピュータに固有のキーデータを使用することで別コンピュータでの該ソフトウエアの不正利用を防止するようにしたものであり、例えばインストールされたソフトウエアを使用する際の不正利用防止、あるいはソフトウエアをコンピュータにインス

トールする際の不正コピー防止などに役立つものである。

【０００２】

【従来の技術】

ソフトウエアの不正使用もしくは不正コピーを防止する従来の技術の代表的なものは、パスワードの入力による方法である。これは、ライセンス提供者から取得した所定のパスワードを入力した場合にだけソフトウエアの使用もしくはコピーを許可する方式である。しかし、この方式では、同じパスワードを用いさえすれば別のコンピュータで同じソフトウエアを使用もしくはコピーすることができるし、また、パスワードは他人に簡単に伝えることができるため、不正コピー防止という意味では明らかに不完全であり、ソフトウエア著作者の権利を保護しきれない。

【０００３】

ソフトウエアの不正コピーをより確実に防止するためにハードウエアキーの方法も用いられている。これは、特定の情報をもったハードウエアを鍵として用いるもので、そのハードウエアがコンピュータに結合されているかどうかを判定してソフトウエアの利用を許可する方法である。キーとなるハードウエアは容易にコピーできないため、この方法によればより確実に不正コピーを防止することができるが、コストが大きいために一部の高価なソフトウエアにしか適用できないという問題がある。また、この方法は、通信ネットワークを介してオンラインで手軽にソフトウエア提供・売買を行なう最近のソフトウエア流通形態には全く不適である。

【０００４】

上記と類似の機能を安価に実現するために、安価な記録媒体を用いた不正コピー防止方法がある。これは、フロッピーディスク等の可搬性の記録媒体に記録した形態でソフトウエアを提供し、インストール実行時に所定のデータを該記録媒体に書き加えることにより、この記録媒体を用いての次回以降のインストールを制限する方法である。しかし、ソフトウエア流通に際しては可搬性の記録媒体に記録された形態をとることを要するため、この方法もまた、通信ネットワークを介してオンラインで手軽にソフトウエア提供・売買を行なう最近のソフトウエア

流通形態には全く不適である。また、記録媒体の読み書き装置を具備していないコンピュータには適用できない、正規のユーザーが該ソフトウエアを再インストールする時に別の新しい記録媒体が必要になる、などの不具合を生ずる。

【０００５】

以上のように、コンピュータを特定する固有情報を利用しない不正コピー防止方法では、それだけでは他のコンピュータへの不正コピーを防止することができない。すなわち、同じ記録媒体やシリアル番号あるいはパスワードなどのキーデータを用いて容易にコピーできるという問題があった。

一方、このような容易な不正コピーを回避する方法としてオペレーティングシステムに固有の情報を利用して不正コピーを防止する方法が考えられている。これは、個別コンピュータのオペレーティングシステム毎に固有のＩＤ番号を付与し、ソフトウエアの側では自己に専用のオペレーティングシステムＩＤ番号を認識しうるよう鍵情報を持ち、該ソフトウエアを利用しようとするコンピュータのオペレーティングシステムのＩＤ番号を該ソフトウエア側の鍵情報を用いて照合することで該ＯＳを具えたコンピュータにおける該ソフトウエアの利用可否を判定するようにしたものである。この方法は上述の従来例に比べて不正コピーを有効に防止することができるが、対象ソフトウエアのプログラムは各オペレーティングシステム毎に異なったプログラムとして作成されねばならないので、ソフトウエアの作成手間がかかるという問題がある。加えて、最近流通してきている異なるどんなＯＳでも動作しうる「クロスプラットホーム」タイプのソフトウエアには適用することができない、という問題がある。

【０００６】

【本発明が解決しようとする課題】

本発明は上述の種々の不具合若しくは問題を解決するためになされたもので、ハードウエアキーや可搬性記録媒体を必要とすることなく、また、オペレーティングシステムの制限を受けることなく、ソフトウエア処理だけで、対象とするソフトウエアの不正利用を防止しうる方法及び該方法に係るプログラムを記憶した記憶波媒体を提供しようとするものである。

【０００７】

【課題を解決するための手段】

本発明に係るソフトウエア不正利用防止方法は、ユーザーのコンピュータのファイルシステムの特徴を検出し、検出したファイルシステムの特徴に基づき固有情報を生成する第１のステップと、前記第１のステップで生成した固有情報に基づきソフトウエアのライセンス提供者の側でキーデータを生成し、該キーデータを前記ユーザに提供する第２のステップと、前記ソフトウエアを利用しようとするコンピュータのファイルシステムの特徴を検出し、検出したファイルシステムの特徴に基づき固有情報を生成する第３のステップと、前記キーデータに対応する前記ファイルシステムの特徴に基づく固有情報と前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報との一致若しくは類似性に基づき前記ソフトウエアの利用可否を判定する第４のステップとを具備する。

一例として、前記ユーザに提供された前記キーデータから前記ファイルシステムの特徴に基づく固有情報を復元するステップを具備し、前記第４のステップでは、前記復元されたファイルシステムの特徴に基づく固有情報と前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報とを比較し、両情報の一致若しくは類似性に基づき前記ソフトウエアの利用可否を判定する。

【０００８】

本発明に係る方法の概略を説明する。

まず、ユーザーに対して固有のキーデータを発行するための前段階の処理として、該ユーザーが使用する特定のコンピュータのファイルシステムの特徴を検出し、検出したファイルシステムの特徴に基づき固有情報を生成する（第１のステップ）。このユーザーとは、例えば対象とするソフトウエアを正規に購入した若しくは購入の意志を示した者である。コンピュータのファイルシステムの特徴の検出は、例えば、コンピュータのファイルシステム情報を読み取ることにより行える。このファイルシステム情報は、個別のコンピュータ毎に固有の、いわば「指紋」のような、情報である。つまり、或るユーザーのコンピュータ（特定のコンピュータ）のファイルシステムは、そのユーザーに特有のファイル使用履歴を示しており、これを固有情報として利用することができる。この第１のステップは、コンピュータのファイルシステムの特徴を検出する（例えばファイルシステ

ム情報を読み取る）処理で済むため、純ソフトウエア処理で遂行でき、特別のハードウエアキーや可搬性記録媒体が不要である。

【０００９】

ユーザー側のコンピュータで読み取られたファイルシステム情報に基づく固有情報は、通信ネットワークを介して、あるいはその他任意の手段を介して、ソフトウエアのライセンス提供者に渡される。ソフトウエアのライセンス提供者の側では、該ファイルシステムの特徴に基づく固有情報に基づき、固有のキーデータを生成する（第２のステップ）。例えば、所定の暗号化アルゴリズムに従って該ファイルシステムの特徴に基づく固有情報を変換することで固有のキーデータを生成する。生成されたキーデータは、通信ネットワークを介して、あるいはその他任意の手段を介して、ユーザーに提供される。こうして、ライセンス提供者によってユーザーに対して上記キーデータが発行されることにより、該ユーザーがオーソライズされる（いわばユーザー登録がなされる）。

【００１０】

ユーザー側では、ソフトウエアを利用しようとするコンピュータのファイルシステムの特徴を検出し、該検出したファイルシステムの特徴に基づき固有情報を生成する（第３のステップ）。このファイルシステムの特徴の検出も、例えばコンピュータのファイルシステム情報を読み取ることにより行える。ここで、以下、読み取ったファイルシステム情報に基づく固有情報を、便宜上、「現在のファイルシステム情報」ということにする。ここでいう「現在」とは、厳密な今の時点であることを要せず、今よりも適宜前の時点（ただし上記キーデータ作成時以降）でのファイルシステム情報であってもよい。

【００１１】

ユーザー側では、前記キーデータに対応する前記ファイルシステムの特徴に基づく固有情報と前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報（つまり「現在のファイルシステム情報」）との一致若しくは類似性に基づき前記ソフトウエアの利用可否を判定する（第４のステップ）。この場合、ユーザ側では、提供されたキーデータから前記ファイルシステムの特徴に基づく固有情報を復元するステップを具備するとよい。この復元は、例えば、前

記所定の暗号化アルゴリズムの逆変換を行なうことにより、行なえる。その場合は、前記第４のステップでは、前記復元されたファイルシステムの特徴に基づく固有情報と前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報とを比較し、両情報の一致若しくは類似性に基づき前記ソフトウエアの利用可否を判定することになる。別の例として、前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報（つまり「現在のファイルシステム情報」）をキーデータに変換し、前記第４のステップでは、前記提供されたキーデータと変換したキーデータとを比較することで、前記ソフトウエアの利用可否を判定するようにしてもよい。要は、ファイルシステムの特徴に基づきソフトウエアの利用可否を判定を行うようになっていればよい。

なお、ユーザ側では、ライセンス提供者から提供されたキーデータを適宜保存しておき、保存したキーデータに基づき該ファイルシステム情報に基づく固有情報を復元するようにするとよい。しかし、ユーザー側でのキーデータの保存は必ずしも必須ではなく、例えば必要なときにライセンス提供者から提供を受けるやり方もあり得る。

【００１２】

例えば、キーデータ作成時つまり登録時からみて、ユーザー側のコンピュータのファイルシステム情報に変更がなければ、両ファイルシステム情報が一致する。これは、ユーザー側の現在のコンピュータが、登録時のキーデータ作成の元となったファイルシステム情報に係るコンピュータと明らかに同一であることを意味する。よって、ソフトウエアの利用を許可するのは勿論である。例えば、ユーザー登録時に続けてこの第４のステップを実行する場合がそのような完全一致のケースに該当する。

ユーザー側のコンピュータの使用に伴ってそのファイルシステム情報の内容が当然変わってくる。そのような場合、前記キーデータから復元されたファイルシステム情報と前記第３のステップで検出された「現在のファイルシステム情報」とは相違してくるが、前記第４のステップでは両者の相違が許容範囲内であれば、類似性を認め、ユーザー側で使用するコンピュータに変わりがないと認定して、ソフトウエアの利用を許可する。一方、登録時にオーソライズされたコンピュ

ータ（キーデータを作成する元となったファイルシステム情報に係るコンピュータ）以外の他のコンピュータで当該ソフトウエアを利用しようとするときには、前記第３のステップで検出された「現在のファイルシステム情報」は、当該他のコンピュータのファイルシステム情報であるから、前記キーデータに基づき復元したファイルシステム情報とは、かなり相違する。よって、前記第４のステップでは両者に一致又は類似性がない、つまり両者の相違が許容範囲外、と判定し、ソフトウエアの利用を不可とする。

【００１３】

このように、本発明によれば、ユーザー側の個別コンピュータに固有の情報として該コンピュータのファイルシステム情報に着目し、該ファイルシステム情報に基づき個別コンピュータに固有のキーデータを作成して、ソフトウエアを利用しようとするコンピュータにおけるファイルシステム情報を該キーデータを用いて評価することでその利用の可否を判定するようにしたので、完全なソフトウエア処理ベースで不正利用を防止することができ、通信ネットワークを介して流通するソフトウエアの不正利用防止対策として最適であり、また、ハードウエアキーが不要であり、格別の可搬性記録媒体の形態で対象ソフトウエアを提供しなければならないような面倒もなく、ローコストであり、ソフトウエア提供者の側において各オペレーティングシステム毎に対象ソフトウエアを作成しなければならない面倒もなく、更には、オペレーティングシステムによる制限を受けないので「クロスプラットホーム」タイプのソフトウエアにも適用することができる、等々の優れた効果を奏する。

【００１４】

なお、コンピュータにおけるソフトウエアの利用とは、様々な利用形態を全て含む。例えば、①ソフトウエアをコンピュータにインストールすること、②インストールされたソフトウエアをコンピュータで起動して、実際にそのプログラムを実行すること、あるいは、③ソフトウエアをコピーすること、などがある。よって、前記第４のステップにおける利用可否判定は、例えば、①ソフトウエアをコンピュータにインストールするとき、あるいは、②ソフトウエアをコンピュータで起動するとき（ソフトウエアのプログラムをスタートするとき）、あるいは

、③ソフトウエアをコピーしようとするとき、のいずれか少なくとも１つの時点で実行すればよい。ここで利用不可と判定されたならばその利用を禁止する、つまり、①インストール処理を中止する、あるいは、②当該ソフトウエアの起動を禁止する、あるいは、③ソフトウエアのコピーを禁止する。通常は、①インストールの禁止と②ソフトウエアの起動禁止とを行なえば、仮りにコピーは可能であったとして、該ソフトウエアの不正利用を差し止めることができるので、上記①インストールの禁止と②ソフトウエアの起動禁止の少なくとも一方を行なえば十分である。勿論、これに限らず、③ソフトウエアのコピーを禁止することのみを行なっても、ソフトウエアの不正利用を防止する効果をあげることが可能である。要するに、前記第４のステップにおける利用可否判定は、どのような時点で行なっても、それなりに、本発明に特有の効果を奏することができる。

【００１５】

また、第４のステップで行なうファイルシステム情報の比較法には種々の手法がありうるので、適宜の手法を採用してよい。一例として、個々のファイルの一致／不一致を比較・判定し、その一致／不一致の度合いからファイルシステム情報全体としての類似度合いを判定する。かかる判定を計量的に行なう一手法として、両ファイルシステム情報の差分若しくは不一致の関数値を計算し、この差分若しくは関数値の大きさに応じて前記ソフトウエアの利用可否を判定する。別の手法としては、パターン認識的手法により両ファイルシステム情報の類似性を判定することが可能である。

【００１６】

ところで、ソフトウエア提供者によってオーソライズされたコンピュータであっても、使用に伴ってそのファイルシステム情報がどんどん変化してゆく。そのため、そのままでは、キーデータによって復元される元の（ユーザー登録時の）ファイルシステム情報と現在のファイルシステム情報との相違が大きくなり、許容範囲を越えて、非類似と判定されることになりかねない。これに対処するために、現在のファイルシステム情報に適合するように、キーデータの内容を適応更新するとよい。すなわち、ユーザ側のコンピュータにおいてキーデータを保存しておき、前記第４のステップでは、保存されたキーデータを用いて判定処理を行

う（例えば保存されたキーデータから元のファイルシステム情報を復元して、比較処理に用いる）。そして、前記第４のステップで前記ソフトウエアが利用可と判定されたことを少なくとも一つの条件として、前記第３のステップで検出されたファイルシステム情報に適合するように前記保存されたキーデータの内容を更新するステップを更に具備するものとする。第４のステップでソフトウエアが利用可と判定されたことを少なくとも一つの条件とする理由は、正規利用が確認されたときだけ、キーデータの内容を適応更新するためである。更に適宜の条件を付加してキーデータの内容の適応更新を行なうようにしてもよい。例えば、第４のステップでソフトウエアが利用可と判定されるごとに常に更新を行なうようにするのが最善であるが、これに限らず、適当な時間間隔で更新を行なうという条件を付加してもよい。

【００１７】

本発明は、方法の発明として実施できるのみならず、該方法に係るプログラムを記憶した記憶媒体の形態で実施することができる。すなわち、本発明に係るコンピュータ読み取り可能な記憶媒体は、コンピュータのソフトウエアの不正利用を防止する方法を前記コンピュータに実行させるためのプログラムを記憶しており、このプログラムは、ユーザーのコンピュータのファイルシステムの特徴を検出し、検出したファイルシステムの特徴に基づく固有情報を出力する第１のステップであって、これにより、該ファイルシステムの特徴に基づく固有情報が前記ソフトウエアのライセンス提供者に対して送付されて該ライセンス提供者の側で該固有情報に対応する固有のキーデータが生成されることを可能にすることと、前記生成されたキーデータを前記ライセンス提供者の側から受け取る第２のステップと、前記ソフトウエアを利用しようとするコンピュータのファイルシステムの特徴を検出し、検出したファイルシステムの特徴に基づき固有情報を生成する第３のステップと、前記キーデータに対応する前記ファイルシステムの特徴に基づく固有情報と前記第３のステップで生成された前記ファイルシステムの特徴に基づく固有情報との一致若しくは類似性に基づき前記ソフトウエアの利用可否を判定する第４のステップとを具備する。

【００１８】

【発明の実施の形態】

以下、本発明の一実施形態を添付図面に基づき詳細に説明する。

図１は本発明に係るソフトウエアの不正利用防止方法の原理を説明する機能ブロック図であり、ブロック１０はソフトウエアライセンス提供者（以下、ライセンサーという）側のコンピュータシステムを示し、ブロック２０はソフトウエア使用者（以下、ユーザーという）側のコンピュータシステムを示す。

【００１９】

ユーザー側のコンピュータシステム２０においては、周知のようにコンピュータハードウエア２１に適宜のオペレーティングシステム（以下、ＯＳと略称する）２２が搭載され、その記憶装置において種々のプログラムやデータの「ファイル」が蓄積されてファイルシステム２３を構築している。このファイルシステム２３は通常知られているようにディレクトリ階層構造をなしている。ライセンサー側のコンピュータシステム１０においても同様の構成を有するが、重要ではないため、図示を省略してある。

【００２０】

ユーザー側のコンピュータシステム２０におけるブロック２４は、本発明に係るソフトウエアの不正利用防止方法を実現するプログラムの部分であり、該プログラムによって実行される処理を機能ブロックによって概念的に示している。一例として、本発明に係るソフトウエアの不正利用防止方法を実現するプログラムは、①登録プログラムと②プロテクトプログラムとを含んでいる。図１において、概ね、点線矢印は①登録プログラムに従う登録時の処理の流れを示し、実線矢印は②プロテクトプログラムに従うソフトウエア利用時の処理の流れを示している。この①登録プログラムと②プロテクトプログラムは、以下述べる例では別々に構成されるものとしているが、一体的に構成されていてもよい。

【００２１】

図２は、本発明に係る不正利用防止方法の対象となるソフトウエアの構造の一例を、①登録プログラムと②プロテクトプログラムに関連して、示す図である。同図（Ａ）は、①登録プログラムが、対象ソフトウエアとは別途に供給される例を示す。この場合は、①登録プログラムは、対象ソフトウエアを提供するライセ

ンサーの側から、対象ソフトウエアの提供を正規に受けようとする（例えば購入しようとする）ユーザーに対して予め提供される。後述する所定の登録手続が完了してから対象ソフトウエアがユーザーに対して提供される。対象ソフトウエアは、該ソフトウエアの本体である「本体プログラム」と、該ソフトウエアをコンピュータにインストールするときに動作する「インストールプログラム」と、インストール済みの該ソフトウエアを起動させる（実行開始）ときに動作する「起動プログラム」とを含み、②プロテクトプログラムを付属している。この②プロテクトプログラムは、「インストールプログラム」と「起動プログラム」の少なくとも一方によって呼び出されて、インストール時及び起動時の少なくとも一方で本発明に従う不正利用防止処理が実行される。

【００２２】

同図（Ｂ）は、対象ソフトウエアが、②プロテクトプログラムのみならず、①登録プログラムをも付属して具備する例を示す。この場合は、後述する所定の登録手続の前に対象ソフトウエアが提供されることになるが、所定の登録手続を完了させない限りソフトウエアの利用ができないので、特に問題ない。

同図（Ｃ）は、最初に①登録プログラムと②プロテクトプログラムだけがユーザーに対して提供され、後述する所定の登録手続が完了してから対象ソフトウエアがユーザーに対して提供される例を示す。

以下の説明では、図２（Ａ）の例のように、①登録プログラムがまずユーザーに提供され、所定の登録手続が完了してから②プロテクトプログラム付の対象ソフトウエアがユーザーに提供される場合を想定して説明する。なお、ライセンサーからユーザーに対するこれらのプログラムあるいはソフトウエアの提供は、通信ネットワークを介してオンラインで行なうことができる。

【００２３】

図３は、本発明に従う不正利用防止方法の第一段階である、ソフトウエア利用登録手続の流れを略示するフロー図である。この登録手続は、ライセンサーからユーザーに対して提供された前記①登録プログラムを、ユーザーのコンピュータで起動させることにより、開始される。主に、図３のステップＳ１，Ｓ２，Ｓ４が、ユーザーのコンピュータで前記①登録プログラムによって実行される処理で

ある。ステップＳ３はライセンサーのコンピュータで行なわれる処理である。

この登録プログラムにおいては、まず、ユーザーのコンピュータのファイルシステム情報を読み取り、これを該登録プログラム中で定義される所定の暗号化アルゴリズムに従って暗号化し、これに基づき暗号化された固有情報を生成する（ステップＳ１）。図１における暗号化器２５のブロックは、この暗号化処理を概念的に示すものである。暗号化アルゴリズムはどのようなものでよい。

【００２４】

周知のように、コンピュータのファイルシステムとは、コンピュータの中のファイルの階層的な構造のことを指す。たとえばWindows（マイクロソフ社の商標）では、プログラムExplorer（マイクロソフ社の商標）を用いてこのファイルシステム情報を読み取り、その階層的構造を視覚的に表示することができる機能を有しているので、そのような既存のファイルシステム情報読み取り機能を利用することができる。また、プログラミング言語のファイルＩ／Ｏの機能を利用してファイルシステム構造を読み取ることができるので、これによってファイルシステム情報を得ることができる。図４にファイルシステムの例を示す。Ｃドライブの中に、「古いメール」などのフォルダがあり、さらにその中に、「○○商事打ち合わせ」など適宜の名称のつけられた各種のファイルが配置されている。この例からも判るように、個別のコンピュータは個々のユーザーによって異なった仕方で用いられるため、家庭もしくはオフィスで通常の使用方法をする限り、個々のユーザが使用を重ねることでそのファイルシステムは個別の各コンピュータ毎に特有のものとなる。言い換えると、ＯＳがインストールされた直後などの特殊な場合を除けば、ファイルシステム情報は個別の各コンピュータ毎に固有の情報であるとみなして差し支えない。よって、ファイルシステム情報を個別コンピュータ毎の固有情報として利用し、後述するように、これに基づき個別コンピュータ毎に固有のキーデータを作成することができる。

【００２５】

なお、ステップＳ１で暗号化された固有情報には、ファイルシステム情報のみならず、ファイルシステム以外の他の情報（例えば現在のコンピュータシステムを記述する他の情報）を含んでいてもよい。要するにファイルシステム情報を少

なくとも含むものであればよい。また、ユーザーのコンピュータの全てのファイルシステム情報を使用せずに一部のファイルシステム情報（例えば所定の一部ドライブあるいは所定の１又は複数のフォルダのファイルシステム情報）のみを使用して暗号化された固有情報を生成するようにしてもよく、これも本発明の範囲に含まれる。なお、ステップＳ１での暗号化処理は、後日、不正利用者がキーデータの解読を不正に行なおうとする場合に、その解読を困難にするためである。よって、場合によっては、ステップＳ１での暗号化処理は省略可能である。

【００２６】

次に、生成したファイルシステム情報に基づく暗号化固有情報を、ユーザーからライセンサーに対して送付する（ステップＳ２）。この固有情報の送付は、通信ネットワークを介してオンラインで行なうことが好ましいが、可搬性媒体を介してオフラインで行なうようにしてもよい。

【００２７】

ライセンサーの側では、ユーザーから該ユーザーの使用するコンピュータに固有のファイルシステム情報に基づく暗号化固有情報を受け取ると、所定の変換アルゴリズム（この変換アルゴリズムは暗号化アルゴリズムであることが、不正利用者の解読を防ぐ上で、好ましい）に従って該暗号化固有情報を変換し、キーデータ（正規利用を許可する鍵となるデータ）を生成する（ステップＳ３）。図１における変換器１１のブロックは、この変換処理を概念的に示すものである。こうして、ユーザーの使用するコンピュータに固有のファイルシステム情報に基づきキーデータが作成される。このキーデータは、ライセンサーからユーザーに対して送付され、ユーザでは、受け取ったキーデータを自己のコンピュータに保存する（ステップＳ４）。このキーデータの送付も、通信ネットワークを介してオンラインで行なうことが好ましいが、可搬性媒体を介してオフラインで行なうようにしてもよい。勿論、キーデータをコンピュータに電子的に保存することをせずに、ライセンサーからユーザーに対して通知されたキーデータをユーザが覚えておき、必要なときにコンピュータに入力するようにしてもよい。

【００２８】

こうして、ライセンサーからユーザーにキーデータが渡されることでユーザ登

録手続が完了する。対象ソフトウエアは、このユーザ登録手続の前又は後の適宜の段階でライセンサーからユーザーに供給される。この対象ソフトウエアの供給も、通信ネットワークを介してオンラインで行なうことが好ましいが、可搬性媒体を介してオフラインで行なうようにしてもよい。

【００２９】

次に、本発明に従う不正利用防止方法の第二段階である、上記②プロテクトプログラムの動作例を図５に示す機能フローチャートを参照しながら説明する。このプロテクトプログラムは、ユーザーが対象ソフトウエアを自己のコンピュータにインストールするとき、あるいはインストール済みの該ソフトウエアを起動するときに、該ユーザのコンピュータで実行される。インストール時にこのプロテクトプログラムを起動させる場合は、対象ソフトウエアのインストールプログラムの実行時にこのプロテクトプログラムが呼び出されて実行され、その結果ソフトウエア利用可と判定されたならばインストールを行なうことが許可される。また、インストール済みの該ソフトウエアの起動時（ソフトウエア実行開始時）にこのプロテクトプログラムを起動させる場合は、対象ソフトウエアの起動プログラムの実行時にこのプロテクトプログラムが呼び出されて実行され、その結果ソフトウエア利用可と判定されたならば該ソフトウエア本体の実行を開始することが許可される。このプロテクトプログラムは、インストール時とソフトウエア起動時のどちらか一方に限らず、両方の時点で実行してもよい。

【００３０】

プロテクトプログラムがスタートすると、まず、キーデータを検索し、キーデータが存在するかどうかを判定する（ステップＳＴ１）。このキーデータ検索の手法としては、プロテクトプログラムに従って表示される入力画面においてユーザーによるキーデータの所在場所情報の入力を受け付け、入力された所在場所情報からキーデータを取得する方法、あるいは、あらかじめ指定されたディレクトリを検索してキーデータを取得する方法、あるいは、コンピュータの記憶領域を隅からしらみつぶしに検索することでキーデータを取得する方法、など適宜の手法を用いてよい。ここで、キーデータが存在しないと判定された場合は、対象ソフトウエアの利用を不許可とする（ステップＳＴ２）。

【００３１】

ステップＳＴ１によりキーデータが存在することが確認された場合は、このキーデータを逆変換することによって元の暗号化固有情報を生成する（ステップＳＴ３）。図１における逆変換器２６のブロックは、このステップＳＴ３における逆変換処理を概念的に示すものである。この逆変換器２６における逆変換アルゴリズムは、前記登録手続時におけるライセンサー側の変換処理（図３のステップＳ３又は図１の変換器１１）による変換アルゴリズムの逆であり、これによりキーデータを変換前の暗号化固有情報に復元する。

【００３２】

次に、復元された暗号化固有情報の暗号化を解除（復号）し、元のファイルシステム情報を含む固有情報を復元する（ステップＳＴ４）。図１における復号化器２７のブロックは、このステップＳＴ４における復号処理を概念的に示すものである。復号化器２７における復号アルゴリズムは、前記登録手続時における暗号化処理（図３のステップＳ１又は図１の暗号化器２５）による暗号化アルゴリズムの逆であり、これにより該暗号化固有情報の暗号化を解除して元のファイルシステム情報を含む固有情報を復元する。

【００３３】

一方、ユーザーのコンピュータの「現在のファイルシステム情報」を適宜の時点で読み取り、これに基づき該ユーザーコンピュータの「現在の固有情報」を提供する（ステップＳＴ５）。このステップＳＴ５の処理は、ステップＳＴ１，ＳＴ３，ＳＴ４のいずれかのステップの前で行なってもよい。また、ユーザーコンピュータの「現在のファイルシステム情報」を読み取ることは、さらに前の適当な時点で行なっておいて、これを保存しておき、保存した「現在のファイルシステム情報」をこのステップＳＴ５で呼び出すようにしてもよい。前述のように、プログラミング言語のファイルＩ／Ｏの機能を利用することで、ファイルシステムの情報を取得することができる。また、このステップＳＴ５で復元するユーザーコンピュータの「現在の固有情報」には、前述のように、ファイルシステム情報のみならず、ファイルシステム以外の他の情報を含んでいてもよく、要するにファイルシステム情報を少なくとも含むものであればよい。また、ユーザーのコ

ンピュータの全てのファイルシステム情報を使用せずに一部のファイルシステム情報のみを使用して暗号化された固有情報を生成するようにしてもよい。ただし、前記登録手続時におけるキーデータ生成の元となったファイルシステム情報を含む固有情報と同じ種類の情報であることを要する。

【００３４】

次に、ステップＳＴ４で得られた「元の固有情報（つまり元のファイルシステム情報）」とステップＳＴ５で得られた「現在の固有情報（つまり現在のファイルシステム情報）」とを比較し、両情報の差分を求める（ステップＳＴ６）。この差分は数値として計算する方法も、ベクトルとして計算する方法も考えられる。たとえば、元の固有情報から得られたファイルシステムに含まれるファイルの集合と、現在のファイルシステムに含まれるファイルの集合をとって、前者と後者の両方に含まれる（一致する）ファイルの個数Ａと、前者または後者のいずれか一方にしか含まれない（一致しない）ファイルの個数Ｂとから、差分Ｃを下記式で計算するやり方が一例として考えられる。

Ｃ＝Ｂ÷（Ａ＋Ｂ）

この差分計算法によると、二つのファイルシステムが完全に一致した場合は、Ｂ＝０であるから、差分Ｃは０となり、最小値をとる。二つのファイルシステムの一方にしか含まれないファイルが増えるほど、Ｂが増すことから、差分Ｃの値が大きくなり、二つのファイルシステムが同名のファイルを一つも含まないときには、Ａ＝０であることから、差分Ｃは最大値である１をとることになる。つまり、差分Ｃは、０から１までの範囲の小数値をとり、その値が０に近いほど一致度／類似度が高い。

【００３５】

次に、比較結果つまり差分Ｃが所定の許容限界を越えているかどうかを判定する（ステップＳＴ７）。図１における比較・判定器２８のブロックは、このステップＳＴ６，ＳＴ７における比較・判定処理を概念的に示すものである。もし、この比較結果つまり差分が許容限界を越えていなければソフトウエアの利用を許可する（ステップＳＴ８）。例えば、実行中のプログラム（インストールプログラムまたは起動プログラム）を続行させる。この比較結果つまり差分が許容限界

を越えているならば、ソフトウエアの利用を不許可とする（ステップＳＴ９）。例えば、不許可のメッセージをコンピュータディスプレイに表示して、プログラム（インストールプログラムまたは起動プログラム）を停止する。

【００３６】

例えば、キーデータ作成時つまり登録時からみて、ユーザー側のコンピュータのファイルシステム情報に変更がなければ、両ファイルシステム情報が一致する。これは、ユーザー側の現在のコンピュータが、登録時のキーデータ作成の元となったファイルシステム情報に係るコンピュータと明らかに同一であることを意味する。よって、ソフトウエアの利用を許可するのは勿論である。例えば、登録時にキーデータを取得した後すぐに対象ソフトウエアをインストールしようとする場合がそのような完全一致のケースに該当する。

一方、ユーザー側のコンピュータの使用に伴ってそのファイルシステム情報の内容が当然変わってくる。そのような場合、ステップＳＴ４で復元された「元のファイルシステム情報」とステップＳＴ５で読み取られた「現在のファイルシステム情報」とは相違してくるが、ステップＳＴ７では両者の相違が許容範囲内であれば、類似性を認め、ユーザー側で使用するコンピュータに変わりがないと認定して、ソフトウエアの利用を許可する。この許容限界値は、ライセンサーが自らの責任で予めプロテクトプログラムに設定しておくものとする。

【００３７】

一方、登録時にオーソライズされたコンピュータ（キーデータを作成する元となったファイルシステム情報に係るコンピュータ）以外の他のコンピュータで当該ソフトウエアを不正にインストール又は使用開始しようとするときには、仮りにオーソライズされたコンピュータの正規のキーデータを知得したとしても、ステップＳＴ５で読み取られた「現在のファイルシステム情報」は、当該他のコンピュータのファイルシステム情報であるから、該正規のキーデータに基づき復元したファイルシステム情報とは、明らかに相違する。よって、ステップＳＴ７では両者に一致又は類似性がない、つまり両者の相違が許容範囲外、と判定し、ソフトウエアの利用を不許可とすることができる。従って、判定の基準となる許容限界値が適切に設定されていれば、ソフトウエアの不正利用を適切に防止するこ

とができる。

【００３８】

ところで、オーソライズされたコンピュータであっても、使用に伴ってそのファイルシステム情報がどんどん変化してゆく。そのため、そのままでは、キーデータによって復元される元の（ユーザー登録時の）ファイルシステム情報と現在のファイルシステム情報との相違が大きくなり、許容範囲を越えて、非類似と判定されることになりかねない。これに対処するために、現在のファイルシステム情報に適合するように、キーデータの内容を適応更新するとよい。

そのために、ソフトウエア利用許可の判定がなされたことを条件に、ステップＳＴ９においてキーデータの適応化更新を行なう。すなわち、ステップＳＴ５で読み取られた「現在のファイルシステム情報」に適合するようにキーデータの内容を更新する。図１における適応化器２９のブロックは、このステップＳＴ９における適応化更新処理を概念的に示すものである。図６は、このキーデータ適応化更新処理の一例を示すフロー図である。利用許可の判定がなされたことを条件にステップＳＴ９０に行き、「現在のファイルシステム情報」に基づき暗号化した固有情報を生成する。この暗号化のために、図３のステップＳ１における暗号化アルゴリズムと同じ暗号化アルゴリズムを用いる。次にステップＳＴ９１では、暗号化された固有情報をキーデータに変換する。この変換のために、図３のステップＳ３におけるライセンサー側の変換アルゴリズムと同じ変換アルゴリズムを用いる。こうして、作成された新しいキーデータによってユーザーコンピュータで保存している古いキーデータを更新するつまり置き換える（ステップＳＴ９２）。利用不可の場合は、ステップＳＴ９０～ＳＴ９２によるキーデータ更新が行なわれない。なお、ステップＳＴ９０では、前のステップＳＴ５で読み取られた「現在のファイルシステム情報」をそのまま使用してもよいし、あるいは「現在のファイルシステム情報」を読み取る処理をあらためて行ってよい。後述するようにこのキーデータ適応化更新処理を任意の時点で行うようにする場合は、このステップＳＴ９０で「現在のファイルシステム情報」を読み取り、読み取った「現在のファイルシステム情報」に基づき暗号化した固有情報を生成する。

【００３９】

キーデータ適応化更新処理はできるだけ頻繁に行ない、適切なキーデータ更新が常になされることが望ましい。対象ソフトウエアの使用起動時にプロテクトプログラムを実行する仕様においては、上記のようにプロテクトプログラム中にステップＳＴ９としてキーデータ適応化更新処理が組み込まれた仕様であれば、該対象ソフトウエアを起動させるたびにキーデータ適応化更新処理を行なうことができる。その場合にあっては、対象ソフトウエアが頻繁に使用するソフトウエアであるならばキーデータ適応化更新処理が比較的十分に行なわれることになる。しかし、対象ソフトウエアが頻繁に使用しないソフトウエアである場合には、キーデータ適応化更新処理を実行する回数が不足し、該ソフトウエアを使用しない間にファイルシステムが大幅に変化することが大いにありうるので、キーデータに対応する古い固有情報（ファイルシステム情報）が現在の固有情報（ファイルシステム情報）と著しく異なることとなり、正規のユーザーに対して使用不許可の判定が下されるおそれが出て来る。一方、対象ソフトウエアのインストール時にのみプロテクトプログラムを実行する仕様においては、上記のようにプロテクトプログラム中にステップＳＴ９としてキーデータ適応化更新処理が組み込まれた仕様のみでは、キーデータ適応化更新処理の実行が不足する。

【００４０】

以上のようなキーデータ適応化更新処理の実行の不足に対処するために、コンピュータでＯＳを起動するたびに、もしくは一定時間ごとに、その他適宜の時点で、図６に示されるキーデータ適応化更新処理を実行するようにすればよい。その場合、最新のソフトウエア利用可否判定結果を記憶しておき、最新の判定結果が利用可の場合にのみ、ステップＳＴ９０～ＳＴ９２のキーデータ更新処理を行なうようにすればよい。具体的には、このキーデータ適応化更新処理を実行するプログラムをコンピュータの起動時に自動的に実行されるプログラムのリストに加えておけば十分である。たとえば、Windows（マイクロソフト社の商標）ではスタートアップファイルとして登録しておけばよい。

【００４１】

本発明に係る不正利用防止方法においては、使用可と判定する前記許容限界の範囲を広くとりすぎると、不正ユーザーを誤って正規ユーザーと認識する可能性

がある。逆に、前記許容限界を狭くとりすぎると、ファイルシステムに急激な変更を加えた場合に、正規ユーザも誤って不正と認識される可能性が高まる。また、ユーザーサービスのためにキーデータを喪失または紛失した場合にキーデータ再発行サービスを行なうことが考えられるが、そのようなキーデータ再発行サービスを悪用して、悪意あるユーザーが別コンピュータの固有情報を利用してキーデータの再発行を要求し、複数のコンピュータでソフトウエアを不正に利用することも不可能ではない。したがって、本発明に係る不正利用防止方法は、全く完全な不正利用防止防止策を提供するものではない。したがって、本発明に係る方法を有効に実施するためには、ライセンサーが自らの責任において使用可否判定の許容範囲若しくは限界値を適切に設定する必要がある。

【００４２】

ただし、前記のような不都合があっても、容易にコピーできるパスワードによる従来の不正利用防止方法と比較すれば、本発明の方法に格段の防止力がある。たとえば、従来のパスワード方式では口頭あるいは電子メールなどによって誰にも見つかることなく不正に他人にパスワードを教えることが可能であり、容易に多人数に伝わりうる。しかし、本発明に係る不正利用防止方法では、仮りに不正利用者がプロテクトプログラムに誤認識させる目的でファイルシステムに作為を施そうとしたとしても、まず、キーデータに対応するファイルシステム構造を解読した上で、コンピュータのファイルシステムをそれに合わせて改造しなければならず、多大な手間がかかり、到底、引き合わないものとなる。また、メールで不正にキーデータの再発行を要求しようとしたとしても、心理的な敷居は高く、またそのような不正な要求を高い頻度で繰り返せば不正が明らかになる、などの種々の事情からパスワードによる従来の防止方法と比べて、不正コピーが広まる恐れは格段に少ないと考えられる。

【００４３】

以上のように、本発明によれば、ライセンサーが許容限界を適切に設定している場合には、ユーザーがソフトウエアを利用するコンピュータの暗号化固有情報をライセンサーに伝え、正規のキーデータを受け取らない限り当該ソフトウエアをコンピュータで利用することが出来ないので、ソフトウエアの不正利用を有効

に防止することができる。また、正規ユーザーであっても１つのソフトウエアを固有情報の異なる他のコンピュータに対してインストールすることは出来ない。よって、ソフトウエアの不正利用防止効果が大である。

なお、インストール時またはソフトウエア起動時に限らず、ソフトウエアのコピー時に本発明に従うプロテクトプログラムを起動させて、不正コピーを禁止するようにしてもよい。また、インストール時にのみ本発明のプロテクトプログラムを実行するものとし、かつ、キーデータ受領時に連続してインストール処理も行なうものとする仕様も可能であり、そのような仕様にあっては、キーデータ適応化更新処理（ステップＳＴ９、図６）は省略可能である。

【００４４】

なお、図１に示す例では、比較・判定器２８のブロックでは、ファイルシステム情報に基づく固有情報同士（つまり暗号化解除した情報同士）で比較を行っているが、この逆に、検出した「現在のファイルシステム情報」を暗号化及び変換して、それに対応するキーデータを生成し、該生成したキーデータと保存してあるキーデータとの比較（つまり暗号化したデータのままの情報同士の比較）によって、利用可否の判定を行うようにしてもよい。しかし、その場合は、不正利用者によるキーデータの改竄の危険性が高まるので、あまり得策ではない。よって、上記実施例に示したようにファイルシステム情報に基づく固有情報（つまり暗号化解除した情報同士）で比較を行う方が得策である。しかし、不利はあるとしてもキーデータ同士で比較する実施態様も、ファイルシステムの特徴に基づきソフトウエアの利用可否を判定するという本発明の技術思想に含まれるものであり、本発明の範囲に含まれる。

【００４５】

なお、本発明は、必要とあらば、ソフトウエア不正利用防止装置という専用ハードウエアの形態で実施することも可能であり、その場合も本発明に従う効果・利点を享受することができる。よって、本発明に従う不正利用防止方法を専用ハードウエア装置で実現しうるように構成した実施の形態も本発明の範囲に含まれる。

【００４６】

【発明の効果】

以上の通り、本発明によれば、ユーザー側の個別コンピュータに固有の情報として該コンピュータのファイルシステム情報に着目し、該ファイルシステム情報に基づき個別コンピュータに固有のキーデータを作成して、ソフトウエアを利用しようとするコンピュータにおけるファイルシステム情報を該キーデータを用いて評価することでその利用の可否を判定するようにしたので、完全なソフトウエア処理ベースで不正利用を防止することができ、通信ネットワークを介して流通するソフトウエアの不正利用防止対策として最適であり、また、ハードウエアキーが不要であり、格別の可搬性記録媒体の形態で対象ソフトウエアを提供しなければならないような面倒もなく、ローコストであり、ソフトウエア提供者の側において各オペレーティングシステム毎に対象ソフトウエアを作成しなければならない面倒もなく、更には、オペレーティングシステムによる制限を受けないので「クロスプラットホーム」タイプのソフトウエアにも適用することができる、等々の優れた効果を奏する。

【図面の簡単な説明】

【図１】　本発明に係るソフトウエアの不正利用防止方法の原理を示す機能ブロック図。

【図２】　本発明に係る不正利用防止方法を実現するプログラム及び対象ソフトウエアの構造を例示する略図。

【図３】　本発明に係る不正利用防止方法に従う登録手続の一例を示すフロー図。

【図４】　ファイルシステムの一例を示す概念図。

【図５】　本発明に係る不正利用防止方法に従うプロテクトプログラムの一例を示すフロー図。

【図６】　キーデータ適応化更新処理の一例を示すフロー図。

【符号の説明】

１０　ライセンス提供者側のコンピュータシステム

２０　ユーザー側のコンピュータシステム

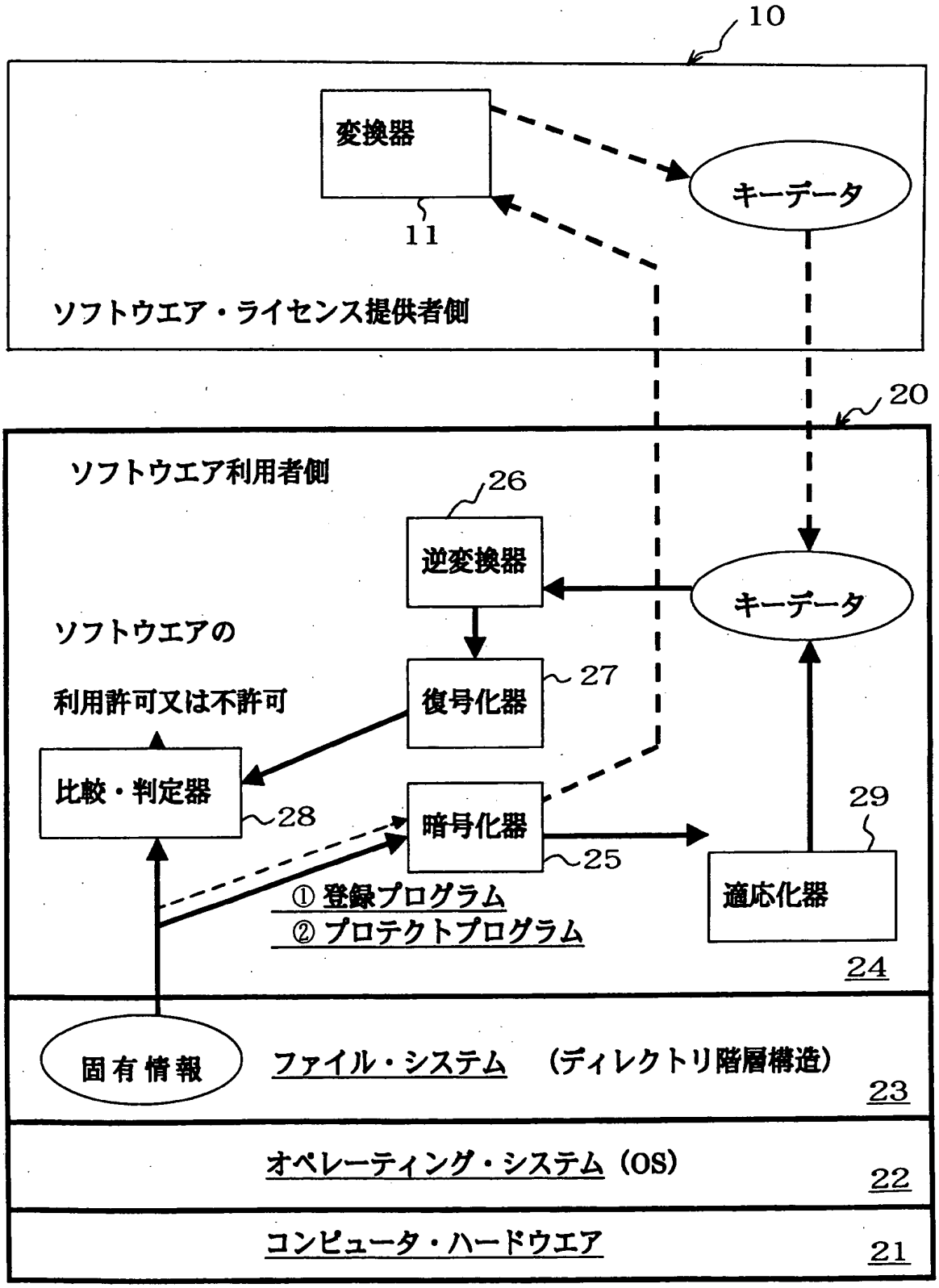
２１　コンピュータハードウエア

２２　ＯＳ

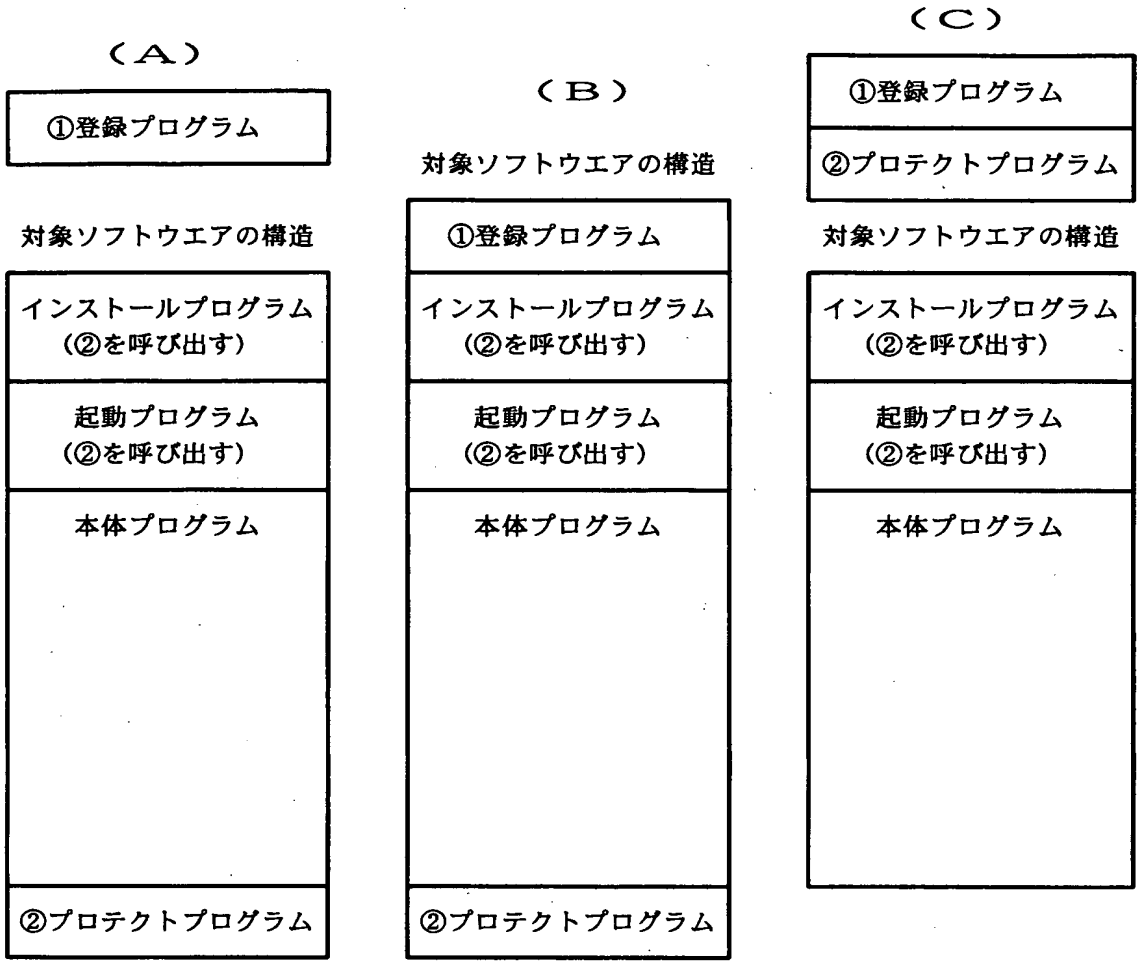
２３　ファイルシステム

【書類名】　図面

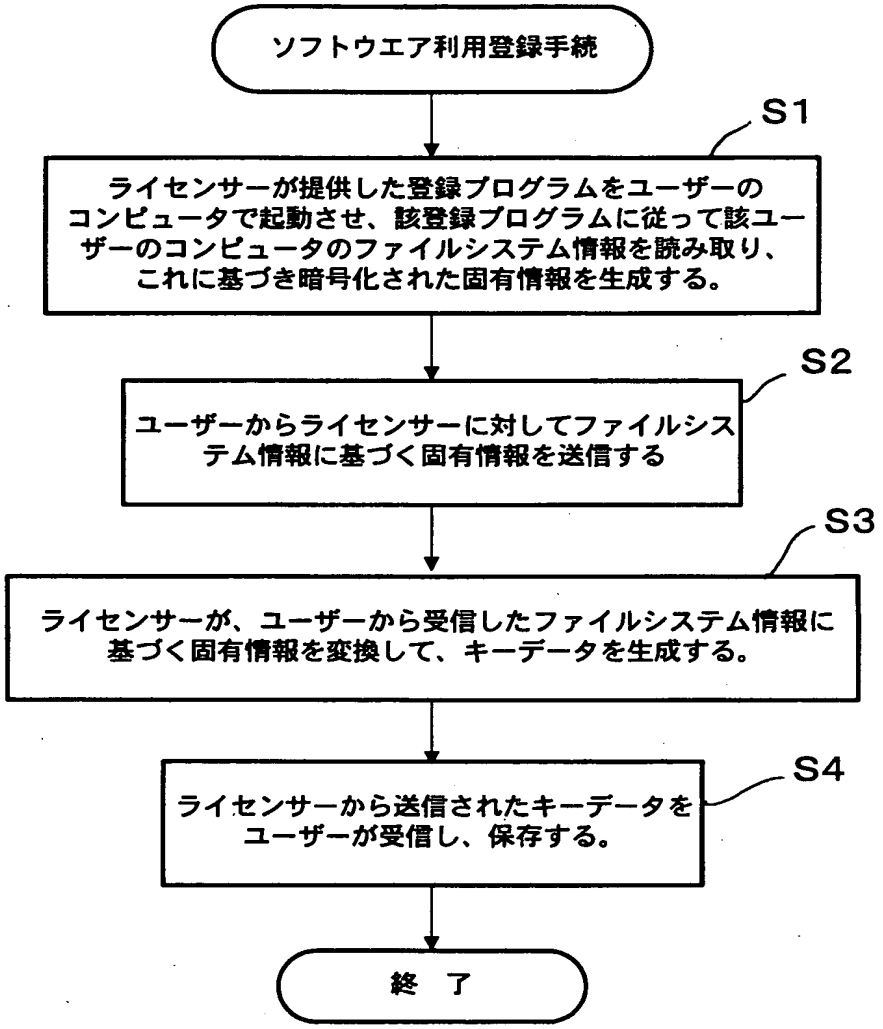
【図１】


10
変換器
11
キーデータ
ソフトウエア・ライセンス提供者側
20
ソフトウエア利用者側
26
逆変換器
キーデータ
ソフトウエアの
利用許可又は不許可
復号化器
27
比較・判定器
28
暗号化器
25
29
適応化器
① 登録プログラム
② プロテクトプログラム
24
固有情報
ファイル・システム　（ディレクトリ階層構造）
23
オペレーティング・システム（OS）
22
コンピュータ・ハードウエア
21

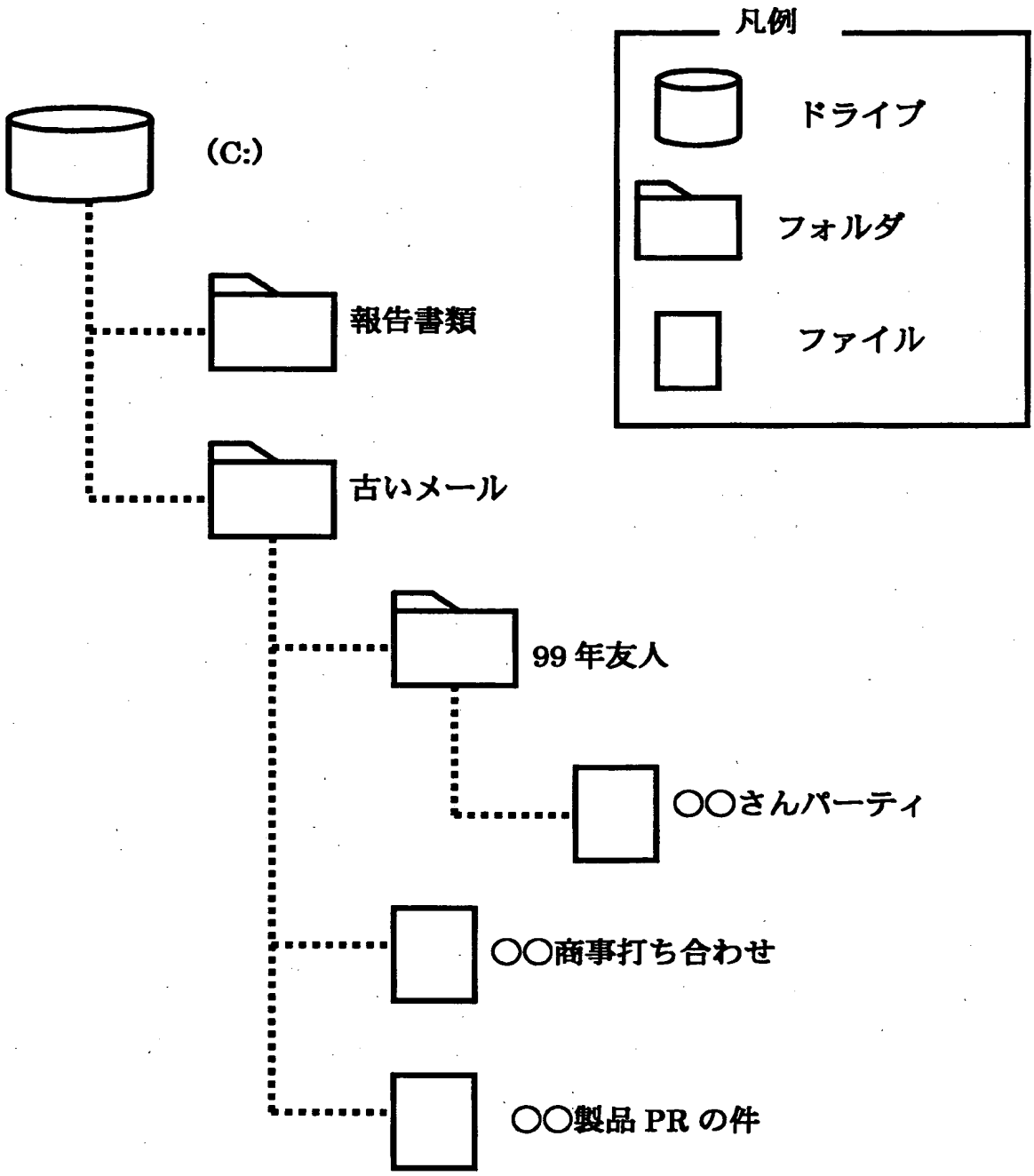
【図２】


（Ａ）
①登録プログラム
対象ソフトウエアの構造
インストールプログラム
(②を呼び出す)
起動プログラム
(②を呼び出す)
本体プログラム
②プロテクトプログラム
（Ｂ）
対象ソフトウエアの構造
①登録プログラム
インストールプログラム
(②を呼び出す)
起動プログラム
(②を呼び出す)
本体プログラム
②プロテクトプログラム
（Ｃ）
①登録プログラム
②プロテクトプログラム
対象ソフトウエアの構造
インストールプログラム
(②を呼び出す)
起動プログラム
(②を呼び出す)
本体プログラム

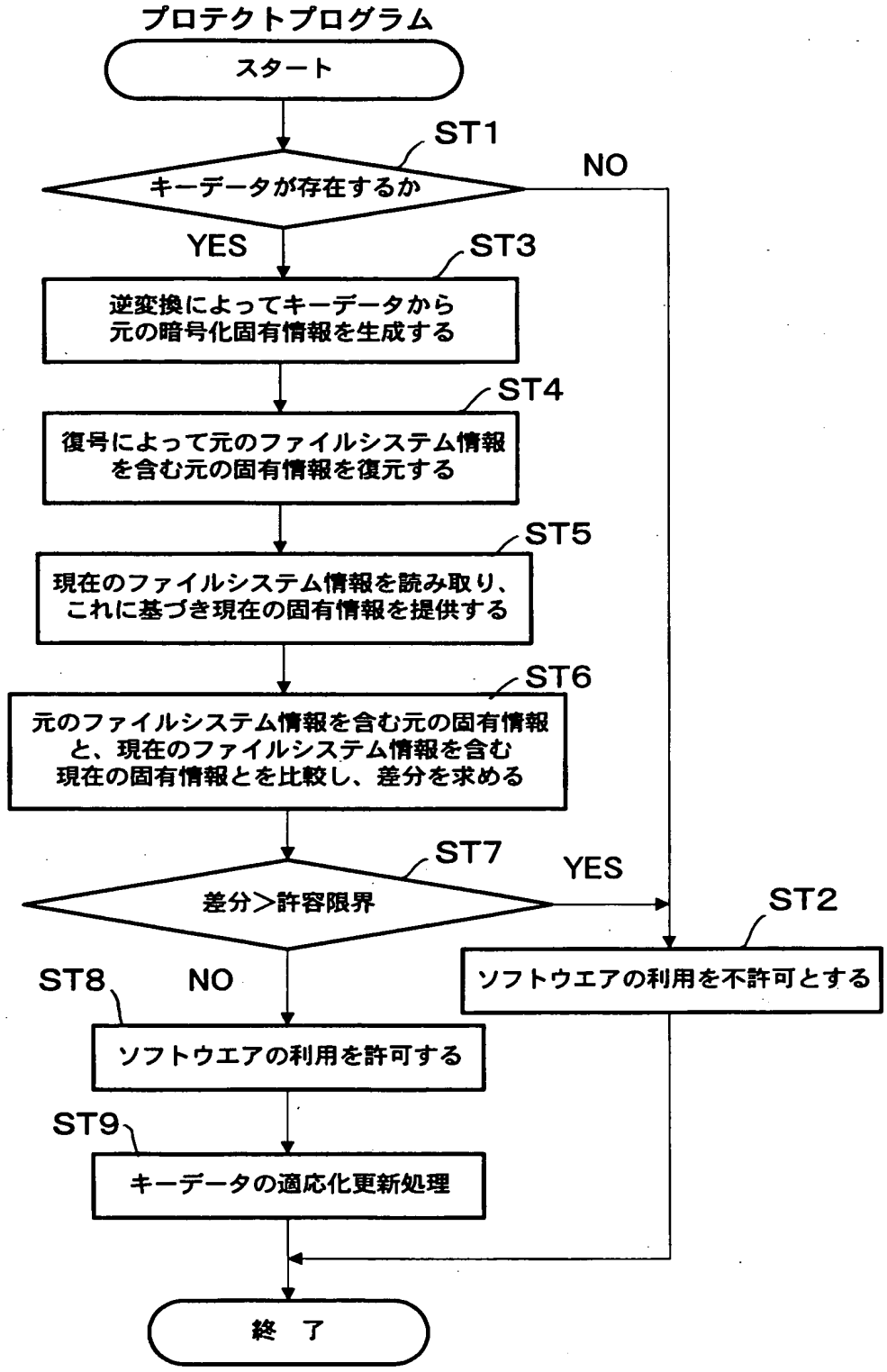
【図３】


ソフトウエア利用登録手続
S1
ライセンサーが提供した登録プログラムをユーザーのコンピュータで起動させ、該登録プログラムに従って該ユーザーのコンピュータのファイルシステム情報を読み取り、これに基づき暗号化された固有情報を生成する。
S2
ユーザーからライセンサーに対してファイルシステム情報に基づく固有情報を送信する
S3
ライセンサーが、ユーザーから受信したファイルシステム情報に基づく固有情報を変換して、キーデータを生成する。
S4
ライセンサーから送信されたキーデータをユーザーが受信し、保存する。
終　了

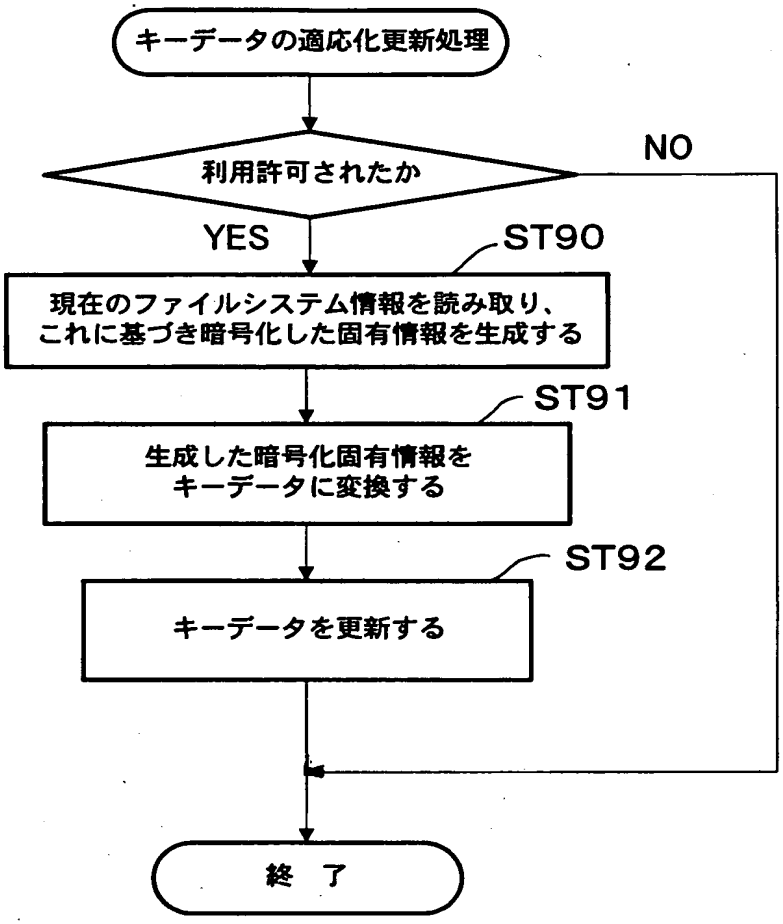
【図４】



【図５】


プロテクトプログラム
スタート
ST1
キーデータが存在するか
NO
YES
ST3
逆変換によってキーデータから
元の暗号化固有情報を生成する
ST4
復号によって元のファイルシステム情報
を含む元の固有情報を復元する
ST5
現在のファイルシステム情報を読み取り、
これに基づき現在の固有情報を提供する
ST6
元のファイルシステム情報を含む元の固有情報
と、現在のファイルシステム情報を含む
現在の固有情報とを比較し、差分を求める
ST7
差分＞許容限界
YES
ST2
ソフトウエアの利用を不許可とする
ST8
NO
ソフトウエアの利用を許可する
ST9
キーデータの適応化更新処理
終　了

【図６】


キーデータの適応化更新処理
利用許可されたか
NO
YES
ST90
現在のファイルシステム情報を読み取り、
これに基づき暗号化した固有情報を生成する
ST91
生成した暗号化固有情報を
キーデータに変換する
ST92
キーデータを更新する
終　了

【書類名】　　要約書

【要約】

【課題】　ライセンサーが許可した特定のコンピュータにおいてのみソフトウエアを利用可能にすることで、該ソフトウエアの不正利用を防止する。このことをＯＳ毎のＩＤ付与やハードウエアキーによらずに純ソフトウエア処理で実現可能とする。

【解決手段】　ユーザーのコンピュータのファイルシステムの特徴を抽出し、これに基づきライセンサーの側で該ユーザーコンピュータのファイルシステムの特徴に固有のキーデータを生成し、ユーザーに付与する。ユーザーコンピュータの側では、対象ソフトウエアのインストール時あるいは使用開始時（起動時）などにおいて、自己のコンピュータのファイルシステムの現在の特徴を読み取り、この現在の特徴と前記キーデータに基づく登録時のファイルシステムの特徴との一致度又は類似性に基づいて、該ソフトウエアの利用の可否を判定する。利用許可されたことを条件に、ファイルシステムの現在の特徴に適合するように、キーデータを更新するとよい。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２０００－３７０６３０
受付番号	５００００１５６９１６７
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年１２月　８日

＜認定情報・付加情報＞

【提出日】　平成12年12月 5日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔５００５５７９１２〕

１．変更年月日　　２０００年１２月　５日
［変更理由］　新規登録
住　所　　神奈川県相模原市古淵一丁目２３番９号
氏　名　　堀　健太